The Digital Operational Resilience Act - (DORA)

HAMMER

BLACK BOX

DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

EU regulation entered into force on 16 January 2023 and will apply as of 17 January 2025.

Enforces strengthening the IT security and operational resilience of financial entities such as banks, insurance companies, investment firms and ICT Vendor.

Lead Overseers can fine providers up to 1% of their average daily worldwide turnover from the previous fiscal year, with daily fines possible for up to six months until compliance is achieved.

Financial institutions should establish compliance with DORA by 2025 through the development and implementation of a robust operational resilience framework.

DORA's main areas are:

- ICT risk management
- ICT incident management and reporting
- **Testing of the operational resilience of ICT systems**
- Management of ICT third-party risks

Over 22,000 financial entities and ICT service providers worldwide will have to comply with DORA.

HAMMER

DORA STATED REQUIREMENTS

Article 21: Financial entities shall test all critical ICT systems and applications at least yearly.

Article 21: Financial entities shall ensure that tests are undertaken by independent parties, whether internal or external.

Article 22: The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with the provisions of Articles 22 and 23.

Article 25: The digital operational resilience testing programme referred to in Article 21 shall provide for the execution of a full range of appropriate tests, including vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, **scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.**

Article 31: It is necessary to establish an appropriate Oversight Framework allowing for **continuous monitoring of the activities of ICT third-party service** providers that are critical ICT third-party service providers to financial entities while ensuring that the confidentiality and security of customers other than financial entities is preserved.

HAMMER

HAMMER CX ASSURANCE

Discover, Deliver, Differentiate

Gain end-to-end CX assurance and support multiple use cases within your customer's communication systems with the Hammer Cloud Platform.

The Hammer Cloud Platform ensures comprehensive assurance throughout the software development lifecycle

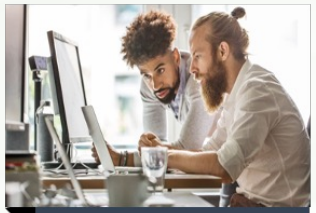
Voice Explorer | Hammer Performance | Hammer QA | VoiceWatch | Virtual Agent

Discover, Assess & Baseline

Discover, assess, and establish a baseline for legacy systems and infrastructure

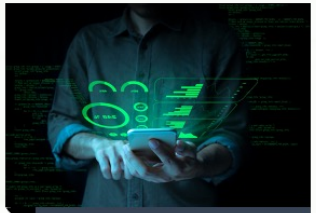
Cloud Migration Assurance

Accelerate cloud migration while ensuring performance standards



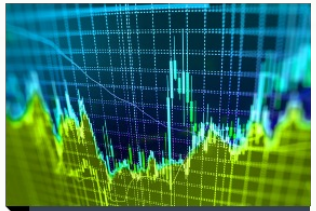
End-to-End Performance

Ensure compliance with regulations, manage risk, and meet SLA requirements



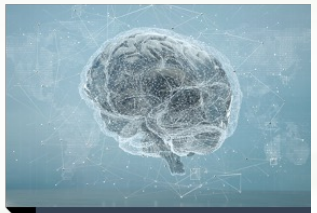
Functional & Regression

Seamlessly integrate third-party applications and perform updates without disruptions



Proactive Monitoring

Detect potential issues in advance and prevent them from becoming critical

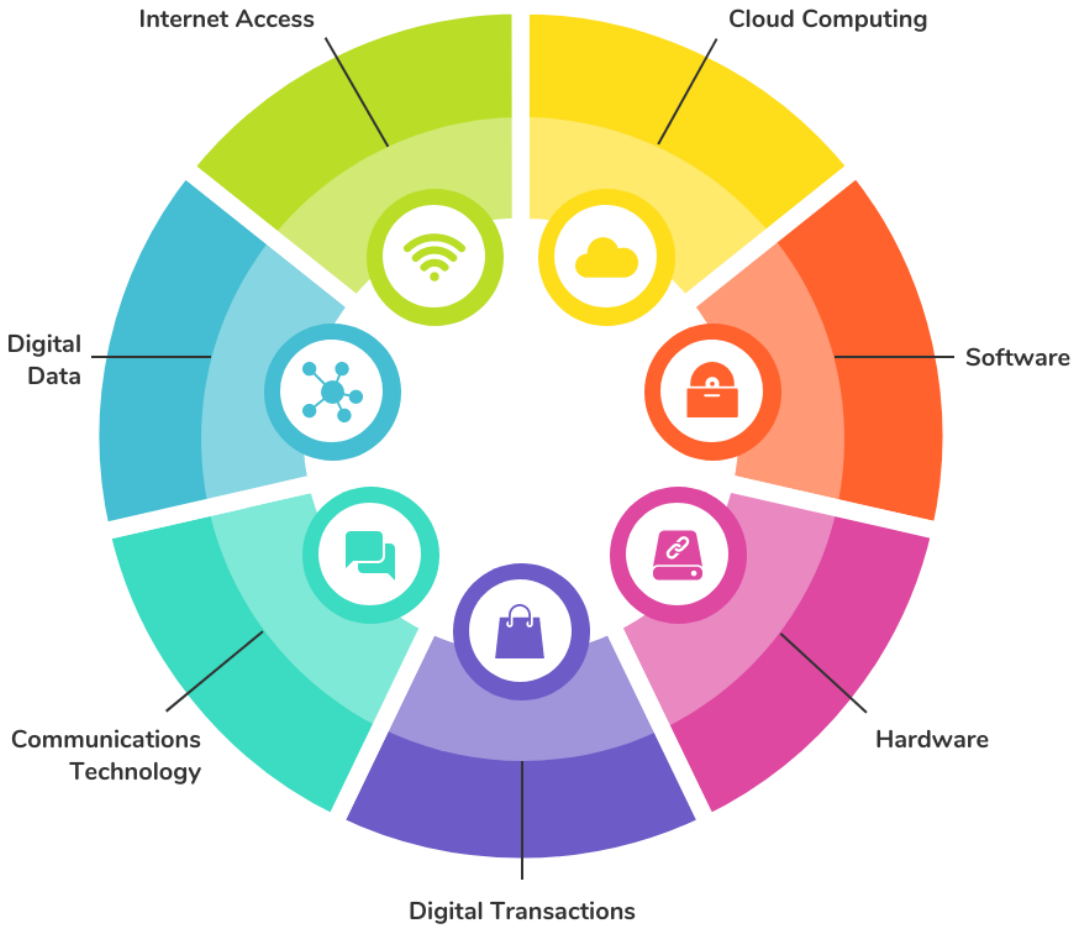


Generative AI Assurance

Ensure the quality, reliability, and ethical considerations of your AI-generated outputs.

Day 1 | Day 2 | Roadmap

Components of ICT



Cloud Computing

The term is generally used to describe data centers available to many users over the Internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers.

Software

Software is a set of instructions, data or programs used to operate computers and execute specific tasks. This is a generic term used to refer to applications, scripts and programs that run on a device.

Hardware

In the context of technology, refers to the physical elements that make up a computer or electronic system and everything else involved that is physically tangible. This includes the monitor, hard drive, memory and the CPU.

Digital Transactions

Digital transactions can be broadly defined as online or automated transactions that take place between people and organizations—without the use of paper.

Communications Technology

Communications technology, also known as information technology, refers to all equipment and programs that are used to process and communicate information.

Digital Data

Digital Data is data that represents other forms of data using specific machine language systems that can be interpreted by various technologies.

Internet Access

Internet access is the process of connecting to the internet using personal computers, laptops or mobile devices by users or enterprises. Internet access is subject to data signalling rates.

HAMMER

Previous Operational Fines Issued

Examples of fines that have been issued to financial institutions for failing to adequately manage their operational resilience:

- In December 2022, the UK Financial Conduct Authority (FCA) and **Prudential Regulation Authority (PRA) fined TSB Bank £48.65 million for operational resilience failings** that led to a major IT outage in April 2018. The outage caused significant disruption to customers, including being unable to access their accounts or make payments. – what was the major IT outage.
- In 2021, the Financial Conduct Authority (FCA**) fined Barclays Bank £26 million for failing to manage its operational resilience adequately**. This was the largest fine ever imposed by the FCA for an operational resilience violation. It is likely that the fines for violations of DORA will be significant, as the regulation is designed to protect the financial system from systemic risks.
- In April 2022, the FCA **fined Raphaels Bank £1.89 million for failing to properly manage its outsourcing arrangements**. The FCA found that Raphaels had inadequate systems and controls in place to oversee its outsourcing providers, which exposed customers to unnecessary and avoidable harm and inconvenience.
- In February 2021, the US Securities and Exchange Commission (SEC) fined the **Commonwealth Bank of Australia $200 million for failing to adequately supervise its foreign exchange trading business**. The SEC found that the bank had failed to implement and maintain adequate risk management controls, which led to significant losses for its customers.
- In January 2021, the Australian Prudential Regulation Authority (APRA) **fined Westpac Banking Corporation $14 million for failing to adequately manage its operational resilience risks**. APRA found that Westpac had failed to implement and maintain adequate systems and controls to prevent and manage operational incidents, which led to a number of outages and disruptions to its customers.

DORA Article's Stating Testing Requirements

Article 21: Financial entities shall test all critical ICT systems and applications at least yearly.

Article 21: Financial entities shall ensure that tests are undertaken by independent parties, whether internal or external.

Article 25: Financial entities shall establish procedures and policies to prioritise, classify and remedy all issues acknowledged throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.

Article 22: The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with the provisions of Articles 22 and 23.

Article 25: The digital operational resilience testing programme referred to in Article 21 shall provide for the execution of a full range of appropriate tests, including vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.

Article 31: It is necessary to establish an appropriate Oversight Framework allowing for a continuous monitoring of the activities of ICT third-party service providers that are critical ICT third-party service providers to financial entities, while ensuring that the confidentiality and security of customers other than financial entities is preserved.

How Hammer Can Support

Hammer's testing and monitoring solutions can support financial institutions in meeting DORA compliance:

ICT risk management

Hammer's solutions can help financial institutions identify, assess, and manage ICT risks by providing them with a comprehensive view of their ICT environment and the threats and vulnerabilities that they face. Hammer’s solutions can also help financial institutions to implement and test their risk management controls. (How do we do this?)

Incident reporting

Hammer’s solutions can help financial institutions report major ICT-related incidents to the competent authorities within a certain timeframe by providing them with real-time monitoring and alerting capabilities. Hammer’s solutions can also help financial institutions to gather and analyse incident data for reporting purposes.

Digital operational resilience testing

Hammer's Testing Platform empowers financial institutions to maintain robust operational resilience and redundancy through comprehensive end-to-end performance and Quality Assurance testing. This enables the identification of vulnerabilities in their ICT infrastructure. Additionally, it facilitates testing in a controlled pre-production environment, ensuring resilience. Moreover, our platform offers continuous monitoring of ICT system performance, promptly alerting you to any irregularities.

ICT third-party risk management

Hammer’s solutions can help financial institutions identify, assess, and manage the risks associated with outsourcing ICT-related services to third parties by providing them with visibility into the third party’s ICT environment and security posture. Hammer’s solutions can also help financial institutions monitor the third party’s performance and identify any potential risks.

In addition to these specific ways in which Hammer's solutions can support DORA compliance, Hammer's solutions can also help financial institutions improve their overall operational resilience posture. This can help financial institutions to reduce the likelihood of ICT incidents occurring and to improve their ability to respond to incidents that do occur.

HAMMER

How Hammer Can Support

Hammer's testing and monitoring solutions are crucial in helping businesses meet compliance in their information communication technology (ICT) systems:

- **Compliance Verification:** Hammer enables businesses to validate and ensure compliance with regulatory standards, industry-specific guidelines, and internal policies. By conducting comprehensive tests and simulations, Hammer can identify any non-compliant areas and help address them proactively.
- **Disaster Recovery Testing:** Hammer's testing solutions can simulate disaster scenarios and assess the effectiveness of your contact centre's disaster recovery plans. By conducting regular tests, businesses can ensure that critical systems and data backups are in place, minimizing downtime and ensuring business continuity in the event of a disaster.
- **Performance and Availability Testing:** Hammer's testing capabilities enable businesses to evaluate the performance and availability of their contact centre systems under different scenarios and workloads. By conducting load testing, stress testing, and capacity planning, Hammer helps identify potential bottlenecks, performance issues, and areas of improvement to ensure optimal system performance.
- **Quality Assurance:** Hammer's testing solutions enable businesses to conduct comprehensive quality assurance testing on their workforce optimisation systems. By creating and executing test scripts, Hammer can verify that the systems are functioning correctly, ensuring accurate forecasting, scheduling, and adherence to service level agreements. Identifying and addressing any issues or discrepancies helps to maintain operational resilience.
- **Compliance and Security Analytics**: Hammer's testing and monitoring solutions help businesses analyse and assess compliance and security-related data. By monitoring compliance metrics, identifying potential security vulnerabilities, and conducting audits, Hammer supports businesses in ensuring adherence to regulatory requirements and maintaining data security.
- **Proactive Issue Detection:** Hammer's monitoring solutions continuously monitor the contact centre environment, detecting and alerting businesses to any anomalies, abnormalities, or potential security breaches. This proactive monitoring helps identify and address issues before they escalate, minimising the impact on compliance and security.

By leveraging Hammer's testing and monitoring solutions, businesses can meet compliance, mitigate risks, and ensure a secure and compliant ICT environment.

QUESTIONS & NEXT STEPS

www.hammer.com

BLACK BOX®

+44 118 965 6088 | BLACKBOX.COM

HAMMER